EXHIBIT C

PART 1

# RealSecure™ Release 1.0
for Windows NT™ 4.0

A User Guide and Reference Manual

Internet Security Systems, Inc.

Visit the ISS Web site at http://www.iss.net

ISS Technical Support: rs-support@lss net

TABLE OF CONTENTS

RealSecure™

Chapter 1: Introduction to RealSecure® for Windows NT

RealSecure is part of Internet Security Systems' SAFEsuite portfolio - a comprehensive line of network security assessment and monitoring tools.

RealSecure is an automatic network attack recognition and response system. It runs on enterprise networks where there is critical data to protect. The system monitors the Ethernet network traffic flow, analyzing the active sessions on the network, and looking for traffic patterns that indicate an attack or unauthorized activity. When an attack is detected, RealSecure can respond automatically to stop the attack before the damage is done.

RealSecure is a network sniffer with an extensive database of attack signatures. It resides on a network segment, analyzing the traffic and looking for attacks in real time When an attack is detected, RealSecure can respond in a number of ways, including:

- recording the date, time, source, and target of the event
- recording the content of the attack
- notifying the Security Administrator
- terminating the attack automatically

RealSecure is completely unobtrusive. It only monitors the local traffic. RealSecure does not add any delay to the network segment.

RealSecure can filter and monitor any TCP/IP protocol. The Security Administrator can configure RealSecure to filter by protocol (TCP, UDP, ICMP), source port, destination port, source IP address, and/or destination IP address. RealSecure can many network services, including web activity, e-mail, file transfer, remote login, chat, talk and a host of others. The range of services that RealSecure can analyze is extended regularly, so be sure to check the ISS Web site at http://www.iss.net for the latest status.

The need for security monitors

"We've put in firewalls, so our network is secure."

This is a common belief in the security industry. Unfortunately, it's not true. Firewalls *are* an important part of a security policy. In fact, they're often the first part of a security policy that a company implements.

But the reality is that firewalls represent only a portion of what's required for complete security policy enforcement. There are a number of additional security threats and situations for which firewalls don't provide an optimal solution:

Most information theft occurs from inside the network. RealSecure can be deployed throughout the network and sees all traffic, not just that which traverses a firewall boundary. Therefore, attacks or unauthorized activity from inside the network is detected. RealSecure's ability to examine Windows networking traffic also helps curtail internal mischief.

Firewalls have tunnels though them and these tunnels can be exploited. RealSecure can detect attacks and unauthorized activity even on legitimate protocols and protocol uses. For example, RealSecure will detect an attempt to gain root access on the FTP server

Network devices like firewalls crash and are sometimes misconfigured. RealSecure sees all the traffic on the network and can detect unauthorized activity that results from firewall or other device misconfigurations. In addition, a burst of activity from RealSecure might be an indication that your firewall has crashed, been misconfigured, or even been compromised.

Administrators are always changing. RealSecure covers an entire subnetwork, regardless of the machines that are on it. Administrators can add, move, and remove machines without worrying about loss of security coverage. RealSecure imposes a very low cost of ownership.

Networks are being used in complex ways. RealSecure looks at TCP/IP and Windows networking traffic and is capable of detecting attacks using these protocols no matter how you are using your network. In addition, RealSecure is updated regularly throughout the year, so that your attack database is as current as possible.

What RealSecure Does

RealSecure was designed to answer these challenges. RealSecure is a "network sniffer" with a unique attack recognition engine including the industry's most extensive database of attack signatures. It sits on a network segment where there is critical data to protect, analyzing the traffic that flows by and looking for attacks in real time. When an attack is detected, RealSecure can respond in a number of ways, including recording the date, time, source, and target of the event, recording the content of the attack, notifying the Security Administrator, and terminating the attack automatically.

How RealSecure addresses security problems

Security Problem	RealSecure Solution
• Most information theft occurs from inside the network.	• RealSecure can be deployed throughout the network to see *all* traffic, not just that which traverses a firewall boundary. Therefore, an attack or unauthorized activity from inside the network is detected. RealSecure's ability to examine Windows networking traffic also helps curtail internal mischief.
• Firewalls have tunnels through them and these tunnels can be exploited.	• RealSecure can detect attacks and unauthorized activity even on legitimate protocols and protocol uses. For example, RealSecure will detect an attempt to gain root access on the FTP server.
• Network devices like firewalls crash and are sometimes misconfigured.	• RealSecure sees all the traffic on the network and can detect unauthorized activity that results from firewall or other device misconfigurations. In addition, a burst of activity from RealSecure might be an indication that your firewall has crashed, been misconfigured, or even been compromised.
• Security Administrators cannot identify the source of an attack.	• RealSecure records the date, time, source, and target of all unauthorized activity, providing critical information that can be used to stop future attacks.
• Networks are always changing.	• RealSecure covers an entire subnetwork, regardless of the machines that are on it. Administrators can add, move, and remove machines without worrying about loss of security coverage. RealSecure imposes a very low cost of ownership.
• Networks are being used in complex ways.	• RealSecure looks at TCP/IP and Windows networking traffic and is capable of detecting attacks using these protocols no matter how you are using your network. In addition, RealSecure is updated regularly throughout the year, so that your attack database is as current as possible.

Cautions and Considerations

Because RealSecure watches and responds to network events, it is a powerful tool, and can be dangerous if used improperly. For example, it can obtain user names, passwords, and e-mail file and transfer information. Exercise caution in the following areas:

RealSecure can log all binary data in a connection, including keystrokes and E-mail. Exercise discretion while using the "Log Raw Data" and "View Session" features. Once logs are created, they should be kept on a secure host, since they often contain passwords or other sensitive data. This is one reason that ISS recommends that the RealSecure Management Console should be run on a dedicated machine. Intruders will perceive the monitoring machine as a prime target, both to steal saved data and to erase evidence of their actions.

RealSecure responds to events. In particular, the "kill" option, if not used carefully, can block traffic over an entire network. Ensure that any network connections being killed are ones that require this action. A wildcard option with a "kill" action stops **all** TCP connections, including HTTP, Telnet and FTP.

To prevent RealSecure from being misused, ISS recommends the following precautions:

- Use the RealSecure Management Console on a dedicated host. Ideally, no other applications should be running on the system.
- Disable all TCP-based services except for TCP/IP. The RealSecure Engine uses UDP and TCP to communicate with the Management Console.
- Ensure that administrator access to the machine is restricted. If possible, disable all other logins.
- Before deploying RealSecure's Engines on the network, scan the system with the ISS Internet Scanner to assess its vulnerability to attack.

About Internet Scanner

Internet Scanner is a security assessment tool that checks all of the network-accessible entities on your network for vulnerability to attack Internet Scanner examines all of the TCP/IP services on your network and includes specific vulnerability checks for Web servers and firewalls.

For more information about Internet Scanner, visit Internet Security System's Web site at http://www.iss.net or send an e-mail message to the ISS Sales Organization at sales@iss.net.

About System Security Scanner

System Security Scanner (S3) is a security assessment tool from Internet Security Systems (ISS). S3 evaluates the security profile of individual UNIX® hosts from the operating system (OS) perspective. S3 complements ISS' Internet Scanner products, which evaluate system vulnerabilities from the outside (across a network). S3 evaluates system vulnerabilities from the inside, from the perspective of the individual host's operating system. S3 assesses file permissions, file ownership, network service configurations, account setup, program authenticity and common user-related security weaknesses such as guessable passwords. S3 also looks for signs that a hacker may have broken into a system.

Your Security Policy
Continuous Security Improvement

A Security Policy is generally a set of rules: Who can access a system and who cannot; which protocols will be permitted on a network and which will not.

RealSecure helps you form and enforce a Security Policy by:

- Allowing you to specify which attacks should be detected and how each one should be handled.
- Allowing you to specify host-specific rules such as permitting connections to certain hosts and denying connection to others.
- Providing audit trails of network activity for evaluating the threats to the Enterprise Network.
- Providing feedback on the effectiveness of your Security Policy
- Allowing you to terminate sessions deemed to be serious threats.

However, they often neglect to mention that "there is not a single solution to Security". Security involves Continuous Security Improvement (CSI).

The Security Cycle

Audit

The illustration above depicts the cycle used to dynamically improve the security of a system. Tools are used to detect the holes in a network. Combining security detection with a security policy establishes the original baseline security

Monitor

A monitoring tool is used to watch for new security breaches or attempts to abuse old holes. This keeps the Security Administrator in touch with the state of the network.

Correct

An essential step of Continuous Security Improvement (CSI) is to monitor and respond to unauthorized access. Measurable feedback is another essential component of the CSI process. Once you have established a security policy and deployed enforcement tools, it is vital that you evaluate how well they are performing. Is my security enforcement meeting my policy expectations? How should my security policy change over time? What new threats and vulnerabilities need to be considered?

RealSecure resides on a networked computer and watches the network traffic. This allows it to compare traffic to a wide variety of attack signatures. It summarizes the information in a concise manner so the security manager can understand what is happening on the network, *as it happens*.

RealSecure and Your Security Policy

A security policy is generally a set of rules regarding system and network access. For example,

- Who can access a system and who cannot.
- Which protocols will be permitted on a network and which will not.
- How new hosts are added to the enterprise network in a controlled manner.

RealSecure helps you form, enforce, and monitor your security policy by:

- Allowing you to specify which attacks should be detected and how each one should be handled.
- Allowing you to terminate sessions deemed to be serious threats.
- Allowing you to specify host-specific access rules, such as permitting connections to certain hosts and denying connections to others.
- Providing audit trails of network activity for evaluating the threats to your enterprise network.
- Providing reports of attacks and responses so that you can evaluate the effectiveness of your security policy.

Legal Issues

In most cases, the United States Government has upheld the right of individuals to monitor their own networks. The general consensus is that all users should be notified of monitoring activities Consult a lawyer if there are any questions as to the legality of using RealSecure on the network. For an explanation of the legal issues, refer to the following CERT advisory:

CA 92:19 CERT

This advisory can be found on CERT's web site:

`http://www.cert.org`

ISS's Adaptive Security Model

Once you have determined your Security Policy, ask Internet Security System's how it's Adaptive Security Model incorporates continuous threat, vulnerability monitoring, response as well as applicable support products being the keys to significant and consistent risk reduction. No other process or technology can, support the following security requirements:

- Ensure all applicable vulnerabilities are removed across the entire network
- Ensure all systems are configured in a secure manner consistent with organizational policy
- Ensure all potentially hostile threats are detected, and responded to in a timely and appropriate manner
- Provide real-time, on-the-fly, technical reconfiguration of threat access routes
- Provide timely security alerts to those responsible for addressing network threats and vulnerabilities
- Provide accurate network security audit analysis data in support of security program planning and assessment efforts

For more information about the Adaptive Security Model and its overall value-added and associated risk mitigation, contact ISS at sales@iss.net or http://www.iss.net.

RealSecure™

Chapter 2: Installing RealSecure for Windows NT

RealSecure has two parts: an engine and a management console. The engine is the low-level software that gathers the packets from the network, looks for attacks, and generates the appropriate response. The Management Console contains the Graphical User Interface (GUI) as well as the collected databases from the engines.

ISS strongly recommends that RealSecure be run on an dedicated system. Not only will this maximize the performance of the engine, but this also protects the system and the data that RealSecure gathers from unauthorized access.

System Requirements

The following sections discuss software and hardware requirements for successfully installing and running RealSecure for Windows NT on the network.

Requirements for Installing RealSecure for Windows NT

Although you can install the RealSecure Engine and Console on the same host, they will usually be installed on different systems. Therefore, the system requirements here are provided for the Engine and the Console separately. If you're installing the Engine and the Console on the same host, just combine the requirements that follow.

System Requirements for the RealSecure Engine:

- 200 MHz Pentium or better
- At least 32 MB of RAM
- At least 100 MB of disk space for the log files and database entries.
- 10 MB for installation of software.
- Windows® NT 4 0.
- An Ethernet card connected to the network segment to be monitored
- In addition, the Administrator of the console host must also have Administrator access privileges on the associated Engine hosts. This is to allow the Console to start and stop each Engine and to push Configuration Templates down to each Engine
- Administrator access privileges to the machine.

***Note:** The Ethernet card must support promiscuous mode.*

System Requirements for the RealSecure Console:

- 200 MHz Pentium or better
- At least 32 MB of RAM
- 100 MB of disk space for each engine that is being managed from the Console.

  ***Note:** ISS recommends that the amount of disk space used for the database will vary greatly. It will depend on how much traffic you see, what you are looking for, what you are writing to the database, and how often you synchronize the database.*

- 15 MB for installation of software.
- Windows® NT 4 0.
- Administrator privileges to the machine.
- Monitor that supports a minimum resolution of 800x600 pixels and 256 colors.

How to determine if you have an evaluation key:

Key files have a text component that can be read with any text editor utility (such as Notepad). You may open a key file with a text editor and look at the contents. You will usually see the term "Evaluation" or "Demonstration" listed in the key's contents However, if your key lists no specific IP addresses, then it is an evaluation key.

Note: *You can also view the key's contents from within the RealSecure Console. Click on "Display Key" from within the "View" menu in the Main Banner Window. That will display the key that RealSecure is currently configured to use.*

What can be done with an evaluation key:

The key for an Evaluation copy of RealSecure for Windows NT (`eval.key`) allows full functionality with the following restrictions:

- Confidential information, including passwords and e-mail data, is replaced with the word "protected" in the decodes and attack signatures.
- Confidential information included in filter actions for "View" and "Log Raw" is replaced with asterisks in the Session Playback view.
- The options to set "kill" and "notify" actions are disabled at the Console and the Engine.
- You may configure and manage only one, local engine from the Management Console.

How to upgrade from an evaluation key:

1. Copy the new key to the RealSecure directory. (Usually c:\Program Files\RealSecure, unless you changed it during installation.)
2. Start the console if it's not already running.
3. Tell the console to use the new key by clicking on:

   View -> Options -> General tab

   Change the field labeled "Key Path" to point to the new key
4. Finally, you also need to push a Configuration Template down to every engine managed by this console. This is because the engines are still stripping out private information and need to be informed that a new key has been loaded. You can push down the same template that an engine is using

Installing RealSecure for Windows NT

Because RealSecure has two components: the Engine and the Console, there are three different installation possibilities:

1. Installing the Engine and the Console on the same host.
2. Installing the Engine only.
3. Installing the Console only.

All three of these can be done with the same installation process. However, before you being installing RealSecure, you should consider which network segments you will be installing RealSecure on, where you'll put Engines, and where you'll put the Management Console.

Note: *The RealSecure Engine can only monitor the traffic that crosses the network segment (or collision domain) on which the Engine is installed. Routers, bridges, switches, firewalls, and smart hubs all will affect the flow of traffic within your network. These devices segment your network into smaller collision domains. Therefore, it is very important that you understand the physical layout of your network when deciding where to place your RealSecure components.*

For example, when a switch receives a packet, it will not broadcast that packet to all of its ports (as a hub will do), but will send the packet only to the port to which the destination device is attached. Switches chop your network into small collision domains. This means that, in a switched environment, a single RealSecure Engine will not see every packet and that multiple Engines need to be deployed.

Installing the Engine and the Console on the same host

To install the RealSecure Engine and Management console on the same host, perform the following steps:

1. Run `setup.exe`, which can be found either on the CD-ROM or in the downloaded archive.
2. After viewing the RealSecure License Agreement, you will see a screen titled "RealSecure Components". Select both the "RealSecure Console" and "RealSecure Engine", then follow the defaults for file assignments.
3. The RealSecure Engine is automatically installed as a Windows NT Service during installation and the output from the Engine is directed to the appropriate log handlers. You can manage the engine through the Windows NT Services Control Panel.
4. Once the installation is complete, you will need to install the ISS Raw Packet Driver v2.0. To do this, perform the following steps:
   a. Open the Network Control Panel.
   b. Select the "Services" tab
   c. Click on the "Add" button.
   d. After the system has compiled its list of known services, click on the "Have disk" button.
   e. The system will prompt you for a location. Enter "`C:\<dir>\driver`", where <dir> is the directory where you installed RealSecure (by default, "`C:\Program Files\RealSecure`").
   f. The system will install a service called "ISS Raw Packet Driver v2.0".
   g. After the installation is complete, you will need to reboot your system for the driver to be loaded properly.

Note: *If you have used the Windows NT version of the ISS Internet Scanner or the Beta version of RealSecure, you may be aware that it also uses a Raw Packet Driver. The packet driver that RealSecure for Windows NT uses is an updated version with better performance. You can distinguish the two by the "v2.0" in the name of the driver. Both versions of the driver can co-exist on the same system although this is not recommended. Since RealSecure uses the 2.0 version of the packet driver, the only situation in which you would need both versions is when you are running both Internet Scanner and RealSecure on the same host. This is not recommended either, for performance reasons.*

5. Once your system has restarted, the next step is to load your key file in the Console's main directory. See Also: Key Information.

6. The final step is to edit the Engine and the Console authentication data, so that both entities can communicate securely. This is discussed in the section titled "Authenticating Engine-Console Communications".

Installing the Console only

To install the RealSecure Management console on a host, perform the following steps:

1. Run `setup.exe`, which can be found either on the CD-ROM or in the downloaded archive.
2. After viewing the RealSecure License Agreement, you will see a screen titled "RealSecure Components". Select the "RealSecure Console" box only, then follow the defaults for file assignments.
3. Once the software has been successfully installed, the next step is to load your key file in the Console main directory. See Also: Key Information
4. The final step is to edit the Console authentication data, so that the Console can communicate with its managed Engines securely. This is discussed in the section titled "Authenticating Engine-Console Communications".

Installing the Engine only

To install only the RealSecure Engine on a host, perform the following steps:

1. Run `setup.exe`, which can be found either on the CD-ROM or in the downloaded archive.
2. After viewing the RealSecure License Agreement, you will see a screen titled "RealSecure Components". Select the "RealSecure Engine" box only, then follow the defaults for file assignments.
3. The RealSecure Engine is automatically installed as a Windows NT Service during installation and the output from the Engine is directed to the appropriate log handlers. You can manage the engine through the Windows NT Services Control Panel.
4. Once the installation is complete, you will need to install the ISS Raw Packet Driver v2.0. To do this, perform the following steps:
   a. Open the Network Control Panel.
   b. Select the "Services" tab.

c. Click on the "Add" button

d. After the system has compiled its list of known services, click on the "Have disk" button.

e The system will prompt you for a location. Enter "`C:\<dir>\driver`", where <dir> is the directory where you installed RealSecure (by default, "`C:\Program Files\RealSecure`").

f The system will install a service called "ISS Raw Packet Driver v2 0"

g. After the installation is complete, you will need to reboot your system for the driver to be loaded properly.

Note: *If you have used the Windows NT version of the ISS Internet Scanner or the Beta version of RealSecure, you may be aware that it also uses a Raw Packet Driver. The packet driver that RealSecure for Windows NT uses is an updated version with better performance. You can distinguish the two by the "v2.0" in the name of the driver. Both versions of the driver can co-exist on the same system although this is not recommended. Since RealSecure uses the 2.0 version of the packet driver, the only situation in which you would need both versions is when you are running both Internet Scanner and RealSecure on the same host. This is not recommended either, for performance reasons.*

5. The final step is to edit the Engine authentication data, so that the engine can communicate with the Console securely. This is discussed in the section titled "Authenticating Engine-Console Communications".

Authenticating Engine-Console Communication

Before you can manage an Engine from the Console, you must authenticate Engine-Console Communications. Authentication validates that a given Console and Engine have permission to talk to each other. Authentication must be completed before the Engines are started, because the "Start" command itself must be authenticated.

Adding an Authentication Entry to an Engine

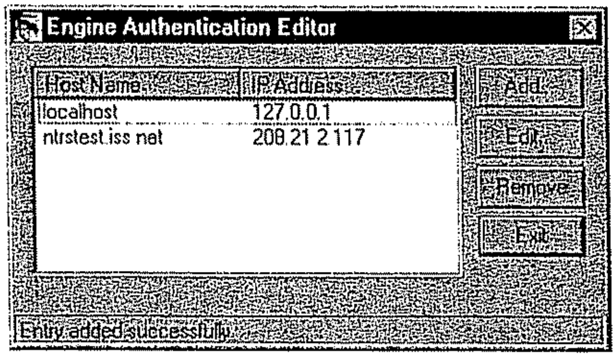
This is done with the "Engine Authentication Editor" which can be found in the "RealSecure" menu in the "Applications" menu from your Start button. This lets you specify which console can communicate with the engine. You will need the following pieces of information

- The IP address (or domain name) of the Console that will communicate with this Engine;
- A passphrase that is used to authenticate communications.

Note: *This passphrase is not transmitted across the network. It is used in combination with an MD5 checksum on each end of the communications.*

Note: *The passphrase is case sensitive and must match exactly what is used on the Console.*

Note: *This procedure must be followed for each RealSecure Engine you have installed.*



Host Name	IP Address
localhost	127.0.0.1
ntrstest.iss.net	208.21.2.117

Entry added successfully.

Figure 1: Engine Authentication Editor

To run the Engine Authentication Editor, double-click on the Engine Authentication Editor in the RealSecure menu in the Applications menu on the Start button.

You will see a list of the Consoles that are authorized to communicate with this Engine. While an Engine may communicate with only one given Console at any point in time, you might want to add other Consoles to this list in case the Engine is moved between management domains sometime in the future.

To add a new entry, click "Add". You'll be prompted for the IP address of a Console that will communicate with this Engine as well as a passphrase to authenticate this communication.

Note: *If you have an active domain name server, you can use the domain name of the Console rather than the IP address.*

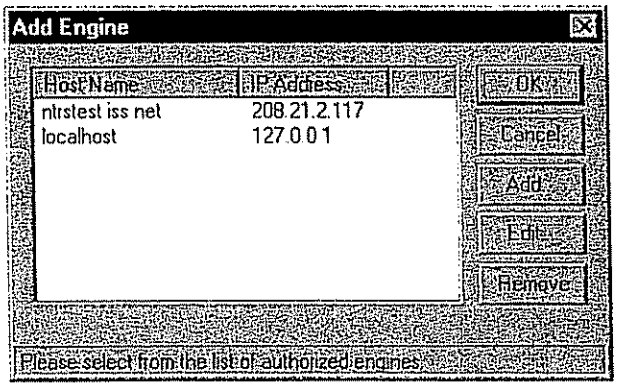
Adding an Authentication Entry to a Console

This is done with the "Add Engine" dialogue, which can be reached from the "New" option in the "Engine" meny from the Engines window in the Console. This lets you specify which Engines will be managed from this Console. You will need the following pieces of information

- The IP address (or domain name) of the Engines that will communicate with this Console;
- A passphrase for each Engine that is used to authenticate communications.

Note: *This passphrase is not transmitted across the network. It is used in combination with an MD5 checksum, on each end of the communications.*

Note: *The passphrase is case sensitive and must match exactly what is used on the Engine.*



Host Name	IP Address
ntrstest.iss.net	208.21.2.117
localhost	127.0.0.1

Please select from the list of authorized engines

Figure 2: Add Engine window

To run the "Add Engine" process, select "New" from the Engine menu in the Engines window.

To add a new entry, click "Add". You'll be prompted for the IP address of a Console that will communicate with this Engine as well as a passphrase to authenticate this communication.

Note: *If you have an active domain name server, you can use the domain name of the Console rather than the IP address.*

The RealSecure for Windows NT Management Console

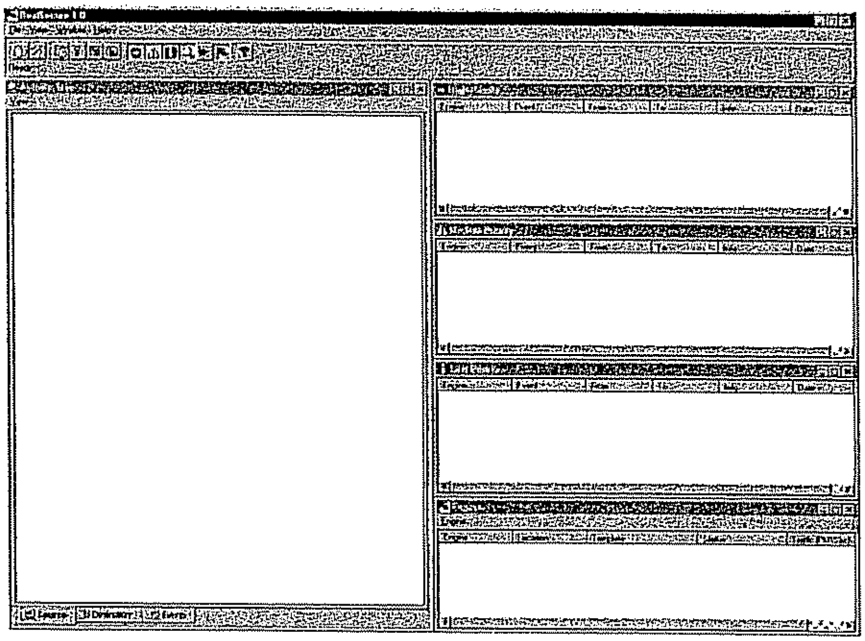


Figure 3: RealSecure for Windows NT Management Console

This is how the RealSecure for Windows NT Management Console appears before any Engines have been added.

RealSecure uses a distributed architecture. The RealSecure engine performs its filtering and monitoring functions on a given network segment. The RealSecure management console displays and logs the data and acts as a centralized engine management point.

RealSecure's Management Console communicates with the RealSecure Engines and includes:

- Start, stop, and pause commands
- Changes to filter rules, attack signatures, and event responses
- Keep-alive checks
- Software updates

There is no hard and fast limitation as to the number of engines that can be controlled by a single RealSecure Management Console. The practical number depends on the following considerations:

- System configuration of the host running the Management Console software
- Amount of traffic that flows between the engine and the console
- Number of attacks and events recognized by the engine

In summary, the number of engines that will normally report effectively to a single console depends on the geographic and organizational limitations of the controlling organization.

See Also: Management Console

Adding Engines to the Console

Before any network data can be logged by the Console, Engines must be associated with the Console. Once Engines are installed on remote machines, they must be added to the Authorization list in Console or Consoles to which they will report. Engines are added to the RealSecure Management Console through the Engine Authorization Editor. For more information about placing Engines on remote machines.

New Engine Dialog Box

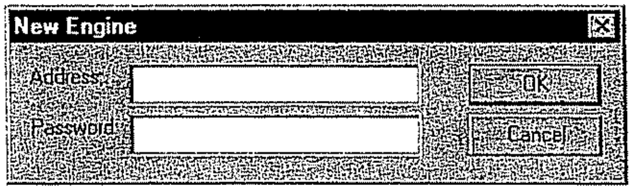


Figure 4: New Engine dialog box

The "New Engine" dialog box associates Engines with the Console. It provides the authentication for the Console to accept data from the Engine. Enter the IP address of the Engine to be added and type a password into the password field

CAUTION!

Passwords can be notoriously easy to steal if they are not highly complex!

Note: *You must run the Engine Authentication Editor for each new Engine you want to add.*

Address: Displays the IP Address for the selected Engine

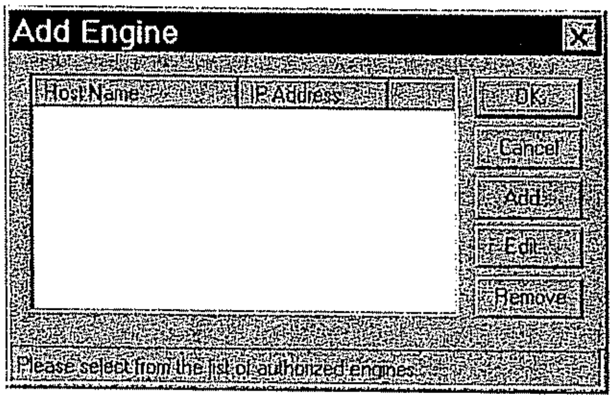
Password: Enter a password here. Remember, passwords are case-sensitive

Note: *You must enter the password in exactly the same form in the Engine Authentication Editor.*

CAUTION!

Passwords can be notoriously easy to steal if they are not highly complex!

Add Engine Dialog Box



Please select from the list of authorized engines.

Figure 5: Add Engine dialog box

Engines can be added, edited or deleted from the Console's authorization list with the Add Engine dialog box. The window displays all Engines present in the Console's authorization list. Once Engines are added to RealSecure, each Engine is listed by machine name and IP address.

Buttons

OK: Click this button to apply a selected Engine to the Console.

Cancel: Click this button to close this dialog without making any changes.

Add: Click this button to open the New Engine dialog box.

Edit: Click this button to change the password and/or IP address for this Engine.

Note: *To change a password, it must be changed at the Engine (through the Engine Authentication Editor) and at the Console.*

Remove: Removes a selected Engine from the list. To remove an Engine, select the Engine to be removed by placing the cursor over the desired Engine and click, then press the Remove button. For more than one engine shift+click for each additional engine, then press the Remove button.

See also: Key Information, Engine Authentication Editor

Start the Engine

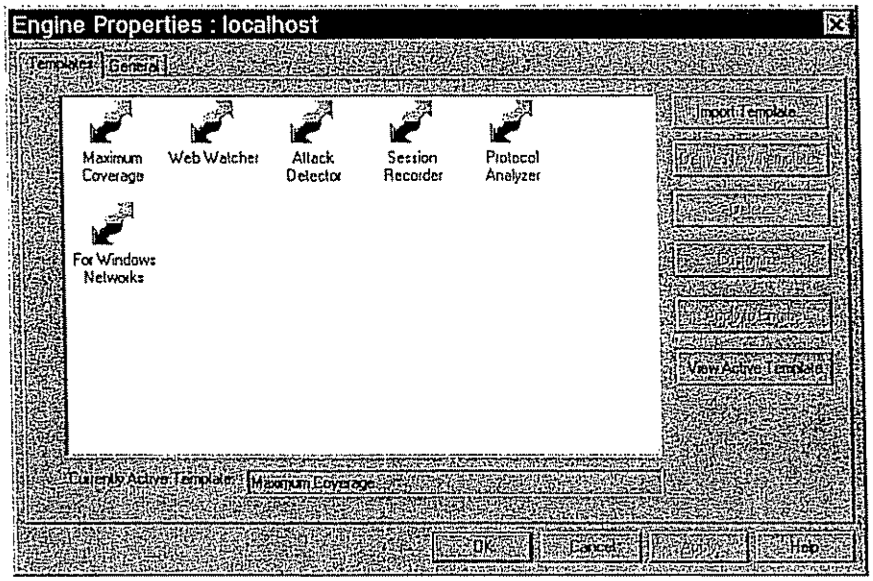
It is important that once you Add Engine/Edit the Console's authentication that you start the RealSecure Engine to ensure it works properly. If you experience any difficulty starting the Engine during this test, contact ISS Technical Support at support@iss net.

Applying a Template

RealSecure for Windows NT uses Templates to configure the Filters and Decodes/Attack Signatures which scan the network. Several default Templates are shipped with RealSecure for Windows NT. To apply a Template to an Engine that has been added to the Console, follow these steps:

1. From the Engines window menu, choose "Properties." The Engine Properties dialog box appears.

Engine Properties Dialog Box



Currently Active Template: Maximum Coverage

Figure 6: Engine Properties dialog box – Templates tab

The Templates tab of this dialog box creates, modifies and assigns Templates.

2. Select the Templates tab (refer to Figure). Choose from one of the pre-configured Templates.

   Note: *ISS recommends beginning with the Maximum Coverage Template.*

3. Click the "Apply to Engine" button. The selected Template is activated on the current Engine, and the "Currently Active Template" field is updated.

Testing the Engine

Depending on the size and speed of the network, data may or may not display the Console immediately. If no information is showing in any of the Console windows, the Engine can be tested by starting an FTP session, checking e-mail, or opening a web browser on the monitored machine. If the ISS Internet Scanner is available, run a scan on the network segment on which the Engine is located. Alerts should display in the Priority windows and entries in the Activity Tree window.

Once Engine-Console communication is functioning properly, RealSecure Engines are ready to deploy on the network

For more information about Engine settings, Templates, and Console configuration, refer to Chapter 3, "Configuring RealSecure for Windows NT".

Engine Window

The Engine Window is used to manage your RealSecure engines. To start an engine, click on the Engine pull-down menu and select "New". As the engine starts up, you will see an MS-DOS window open that displays the progress of the engine as it starts. Minimize this window. Once the engine is running, you will begin to see traffic appearing in the Activity, High, Medium, and Low windows.

RealSecure's engines communicate with the RealSecure Management Console in the following ways:

- **Event** messages are indications that something interesting has occurred. These messages are passed up to the Management Console as they occur.
- **Keep-alive** responses that indicates "I am still alive".
- **Raw Session Data** is the keystroke or data content of a session. This information is passed up to the Management Console as it occurs if the action associated with an event is "View Session".
- **Database and Log file information** are sent up to the Management Console on demand.

Installing Additional Engines

The key determines how many Engines can be installed. See Also: Key Information.

Note: *Use a Domain account with Administrator privileges on each remote machine where and Engine is placed.*

To install an Engine on a remote machine:

1. Run the setup as described previously in this chapter, selecting the "RealSecure Engine" installation option and making sure that "RealSecure Console" is unchecked. Two checkboxes are provided, one for the RealSecure Engine installation option and the other for the RealSecure Console installation option.
2. Run the Engine Authentication Editor and enter a password to add the Engine to the Console's Authentication list.

Note: *ISS recommends that Engines are installed into the same directory on each machine (usually* `C:\Program Files\RealSecure`*). This will simplify maintenance.*

Key Information

RealSecure for NT is keyed to a particular network to prevent product misuse. Before running RealSecure, a key must be obtained. To obtain a License Key File, please contact ISS at (770)395-0150 or by e-mail at keys@iss.net. Upon receiving a license key, save the key as the filename iss.key in the directory RealSecure is installed in.

RealSecure WILL NOT operate without a key. For more information about key processing, send an e-mail message to support@iss.net.

The RealSecure for NT License Key runs on the Management Console. It controls the following parameters:

- Range of IP Addresses on which you can start an Engine
- Number of Engines you can deploy

Keys are valid for a predetermined amount of time. If your key expires, or if you wish to upgrade an Evaluation key, contact your sales representative at sales@iss.net.

RealSecure™

Chapter 3: Configuring RealSecure for Windows NT

Before any network data can be logged by the Console, you must associate an Engine or Engines with the Console. Once you have installed Engines on remote machines, they must be added to the Authentication list in the Console or Consoles to which they will report. The Authentication list keeps track of which Engines are associated with the Console, associates the Engine passwords with the Console, and coordinates your Key file with the Engines in use.

Configuration settings for RealSecure can be grouped into two categories: Console and Engine. All configuration settings are managed from the Console

See also: Installing a Localhost Engine, Installing Remote Engines and The Engine Authentication Editor.

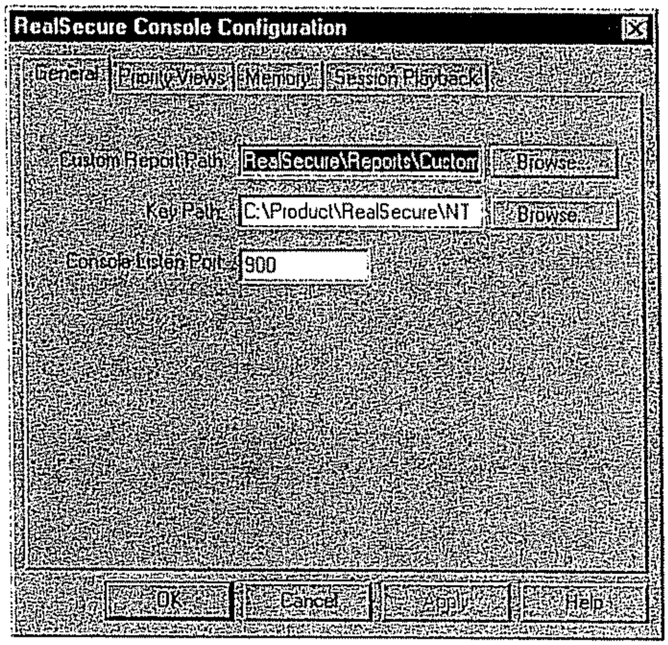
Console Configuration

Console Configuration allows specification of certain critical file paths needed for Engine-Console communication and to set memory options.

Console Configuration Dialog Box

To configure the RealSecure Management Console, click the "Configuration Options" button on the Toolbar, or select "Options" from the Console's View menu. The "Console Configuration" dialog box is displayed. It allows determination of the parameter paths, priority display timeouts, performance parameters, and the Session Playback option.

General Tab



Custom Report Path: RealSecure\Reports\Custom

Key Path: C:\Product\RealSecure\NT

Console Listen Port: 900

Figure 7: Console Configuration dialog box - General Tab

The General tab allows you to specify the custom path to various system configuration parameters.

Custom Report Path: The directory path where reports are to be found. Type the path directly or use the "Browse" button.

Key Path: The path to the ISS Key. Type the path directly or use the "Browse" button. Use this to instruct RealSecure to use a different Key

Console Listen Port: The UDP port on which RealSecure's Management Console listens for messages from the Engines.

Buttons

OK: Saves changes and exits.

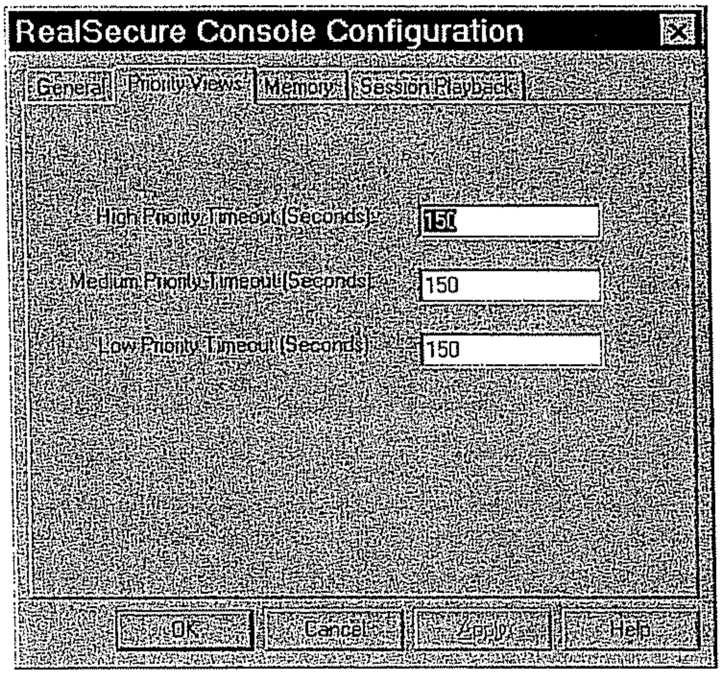
Cancel: Exits without saving changes.

Apply: Applies changes without exiting.

Help: Displays an online help topic for this tab.

Browse: Searches for a directory path or file.

Priority Views Tab



High Priority Timeout (Seconds): 150

Medium Priority Timeout (Seconds): 150

Low Priority Timeout (Seconds): 150

Figure 8: Console Configuration dialog box - Priority Views tab

The Priority Views tab sets the following options:

High Priority Timeout (Seconds): The number of seconds before an event is removed from the Console's High Priority window. The default is 150 (or 2.5 minutes).

Medium Priority Timeout (Seconds): The number of seconds before an event is removed from the Console's Medium Priority window. The default is 150.

Low Priority Timeout (Seconds): The number of seconds before an event is removed from the Console's Low Priority window. The default is 150.

***Note:** The higher the value, the more memory that will be used.*

Buttons

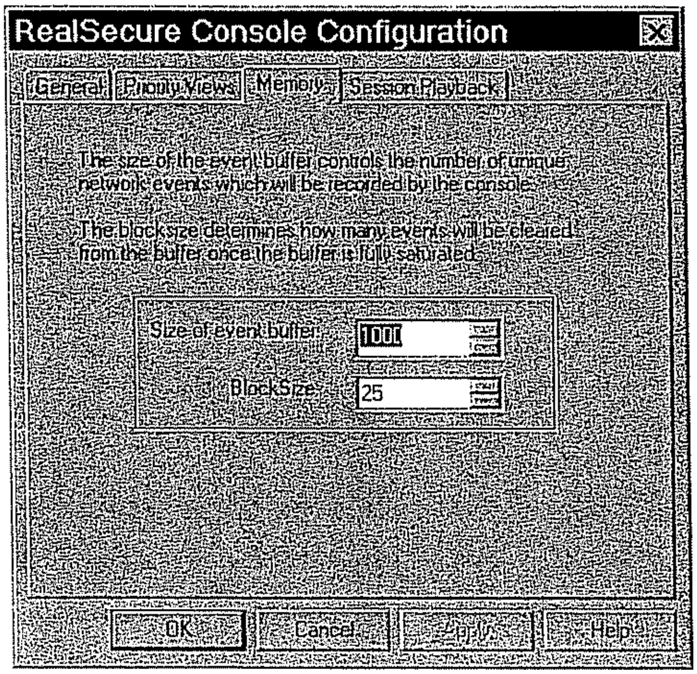
OK: Saves changes and exits.

Cancel: Exits without saving changes.

Apply: Applies changes without exiting.

Help: Displays an online help topic for this tab.

Memory Tab



The size of the event buffer controls the number of unique network events which will be recorded by the console.

The block size determines how many events will be cleared from the buffer once the buffer is fully saturated.

Size of event buffer: 1000

BlockSize: 25

Figure 9: Console Configuration dialog box - Memory tab

The Memory tab allows you to specify some performance related options:

Size of Event Buffer: The number of unique network events which the Console stores at any point in time. Enter the number directly or use the up and down arrows. Once this number is reached, it begins taking out the old ones.

Block Size: The number of events which are cleared from the buffer once it is saturated. Enter the number directly or use the up and down arrows.

Buttons

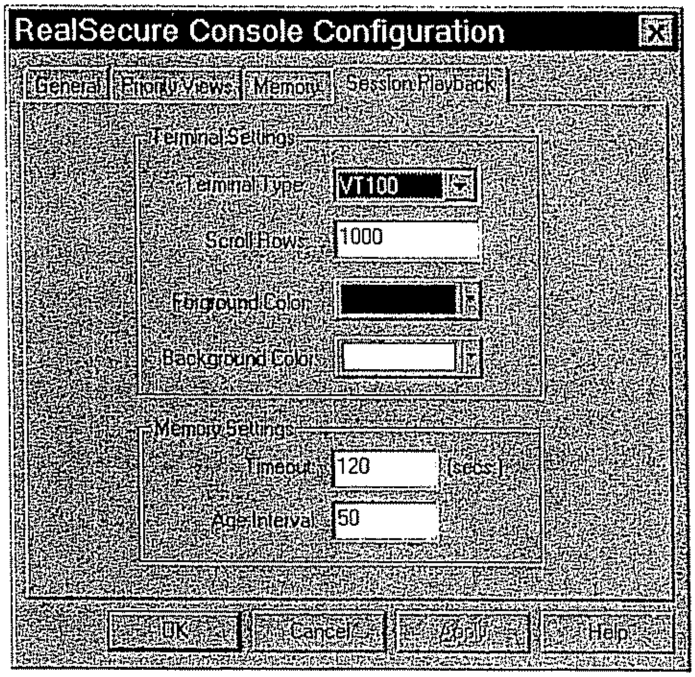
OK: Saves changes and exits.

Cancel: Exits without saving changes.

Apply: Applies changes without exiting.

Help: Displays an online help topic for this tab.

Session Playback Tab



Terminal Type: VT100

Scroll Rows: 1000

Foreground Color: ■

Background Color: □

Timeout: 120 [secs.]

Age Interval: 50

Figure 10: Console Configuration dialog box - Session Playback tab

The Session Playback tab allows for setting the following options:

Terminal Type: Choose the type of terminal emulation for viewing session data. The default is VT100.

Scroll Rows: Type the number of rows of data to keep in the scrollback buffer. The default is 1000.

Foreground Color: The default foreground color (the color of the text) is black. Click in the colored button to select a different background color.

Background Color: The default background color is white. Click in the colored button to select a different background color.

Buttons

OK: Saves changes and exits.

Cancel: Exits without saving changes.

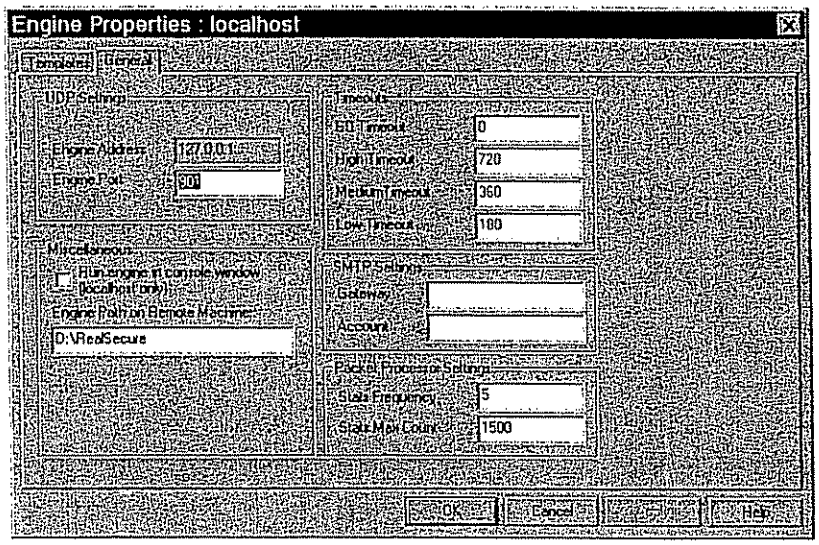
Apply: Applies changes without exiting.

Help: Displays an On-line Help topic for this tab.

Engine Configuration

The Engine Properties dialog box sets certain Engine parameters and e-mail options. It also assigns, modifies, and creates Templates for the Engines through the Edit Template dialog box.

Engine Properties Dialog Box



Engine Properties : localhost

UDP Settings
Engine Address: 127.0.0.1
Engine Port: 901

Miscellaneous
□ Run engine in console window (localhost only)
Engine Path on Remote Machine: D:\RealSecure

Timeouts
EO Timeout: 0
High Timeout: 720
Medium Timeout: 360
Low Timeout: 180

SMTP Settings
Gateway:
Account:

Packet Processor Settings
Stats Frequency: 5
Stats Max Count: 1500

Figure 11: Engine Properties dialog box

The Engine Properties Dialog Box configures RealSecure's Engine and assigns and configures Templates.

Note: *The Engine currently being configured appears in the dialog box title bar.*

General Tab

The following settings are available from the Engine Properties General Tab:

UDP Settings

Engine Address: The IP address of the current Engine.

Engine Port: The UDP port on which the Engine listens for messages from the Console.

Miscellaneous

This checkbox forces the Engine to run as an application rather than an NT Service. The output of the Engine will be displayed in a command window on the desktop rather than in the Event Log.

Note: *This is recommended for debugging purposes only.*

Engine Path on Remote Machine: Displays the path to the currently selected Engine, relative to the machine on which the engine is running.

Timeouts

GC Timeout: The number of seconds TCP stream data is held in memory before "garbage collection" removes it. Higher numbers may require more RAM.

High Timeout: The number of seconds before High Priority events are timed out and removed from the Engine.

Medium Timeout: The number of seconds before Medium Priority events are timed out and removed from the Engine.

Low Timeout: The number of seconds before Low Priority events are timed out and removed from the Engine.

Note: *If the Timeout settings are changed in the Engine Properties dialog box to fewer seconds than the Timeouts in the Console Configuration dialog box, it can result in the same event being reported in the Console more than once.*

SMTP Settings

Gateway: The name of the SMTP server, in the following format:

```
mail.mynet.com
```

Account: The e-mail account name to which notifications are sent.

Packet Processor Settings

Stats: The frequency of seconds between "packet per second" updates.

Stats Max: The expected maximum packet rate (the Engine adjusts if this number is exceeded).

Buttons

OK: Saves changes and exits.

Cancel: Exits without saving changes.

Apply: Applies changes without exiting.

Help: Displays an On-line Help topic for this tab.

RealSecure Template Configuration

RealSecure's Templates control Engine behavior. They specify the following:

- which attacks an Engine detects
- which sessions an Engine decodes
- how an Engine filters packets
- the priority of each network event
- how an Engine responds to network events

There are three types of events in each Template:

- **Attack:** Network activity that indicates an attempt to obtain unauthorized access to the data on the network. By default, attacks are **High Priority** events. When an Engine detects an attack, the default response is to notify the Management Console and log a summary of the event to the database.
- **Decodes:** A network event that does not constitute an attack but which might be interesting to a Security Administrator. Examples include FTP and HTTP sessions. By default, sessions are **Medium Priority** events. When an Engine detects a session of interest, the default response is to notify the Management Console only.
- **Filter:** Filter events represent matches with the low-level RealSecure filtering rules. Since filters can be added by the Security Administrator, they can also indicate interesting network activity. By default, filter events are **Low Priority** events. When an Engine detects a filter event, the default response is to ignore the event. The Management Console is not notified, nor is the event logged to the database.

The Kill response option is only available to TCP filters. Use the "Kill" option very carefully, as it will terminate every connection that matches the criteria. Consider the implications of the kill option very carefully before employing it on the network.

Automatically "Kill" TCP-based Attacks

RealSecure can kill a TCP connection automatically by sending a RST packet to each session participant. A "Kill" can minimize the network's vulnerability to attack. Many attacks can be stopped before damage is done.

Default Templates

Six default Templates are provided, which contain configuration settings for different environments:

Maximum Coverage

With this Template, all the capabilities of the RealSecure Engine are activated. Every attack signature is enabled, every session protocol decode is active. All of the filters that RealSecure normally supports are also active. This is a good Template to start using immediately.

Attack Detector

Using this Template, a RealSecure Engine focuses on network attacks only. Sessions are not decoded and filter events are not reported. On a healthy, secure network, Engines using this Template generate virtually no traffic. This Template is appropriate for administrators who want to know only about the most severe network events.

Protocol Analyzer

This Template is the opposite of "Attack Detector". In this Template, only the session decoding is active. Attack detection is inactive. This Template is appropriate for Security Administrators who want to understand how their network is being used.

Web Watcher

Engines using the "Web Watcher" Template see all the HTTP traffic traversing the local network segment. This Template is appropriate for Security Administrators who want to gain a better understanding of the web traffic on the network. It might also be appropriate for an Engine installed on a segment with web servers only.

Note: *Only the HTTP-based attack signatures are enabled with this Template. Other attack signatures are not active.*

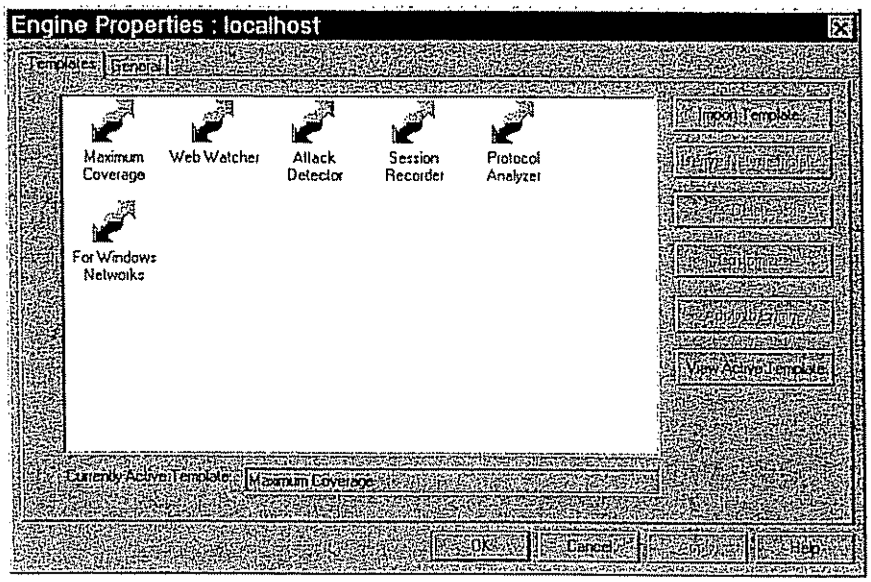
For Windows Networks

This Template includes a collection of attack signatures, session decodes, and filter rules that are specific to Windows networking environments. Several of the attacks that RealSecure can recognize are specific to UNIX systems. If there are no UNIX systems, then these attacks can be disabled. This Template includes signatures for networks that include only Windows devices.

Session Recorder

This Template provides sample filters for recording Telnet, FTP, SMTP (E-mail) and NNTP (NetNews) sessions. In order to record a session, create a filter for each side of the session. This Template provides functional examples.

Templates Tab



Currently Active Template: Maximum Coverage

Figure 12: Engine Properties dialog box - Template tab

Templates are ways to group an Engine's settings into a reusable and resettable package. This allows a user to change the personality of the Engine with minimal effort. The Templates tab displays the Templates which are currently available in the configuration of RealSecure for Windows NT. To access this dialog box, either select "Properties" from the Engine menu in the Engines window or click the "View Engine Properties" toolbar button with an Engine selected.

The main window of this dialog contains Template icons. The name of the active Template for the selected Engine is displayed in the "Currently Active Template" field directly below the main window

***Note:** Some of the templates provided with RealSecure are locked which prohibits accessibility to modify the template. These templates will be shown with a lock displayed next to the template icon.*

Buttons

Import Template: Used to cause RealSecure to recognize a Template from an outside source. Copies the Template into the Template directory if it is not already found there, and adds registry information for the Template If a Template with the same name is found, the system either changes the new Template's name to overwrites the old one

Derive New Template: Creates a copy of the selected Template. Use "Derive New Template" to derive a new template from an existing template. This is one way to create an unlocked version of a locked template. It is also a way to create a completely new template without having to set every setting. This feature enables you to return to the original state of the default "Locked" templates This also displays the "Choose Template Name" dialog box.

Delete: Deletes the currently selected Template.

Customize: Displays the Edit Template dialog box.

Apply to Engine: Applies the currently selected Template to the currently running Engine.

View Active Template: Displays the filters and decodes for the current Template. This displays the current settings on the selected Engine. This can be a great way to determine an Engine's current settings when you are unsure of what the template settings are.

OK: Saves changes and exits this dialog box.

Cancel: Exits without saving changes.

Apply: Applies changes without exiting.

Help: Displays an On-line Help topic for this tab.

Choose Template Name Dialog Box

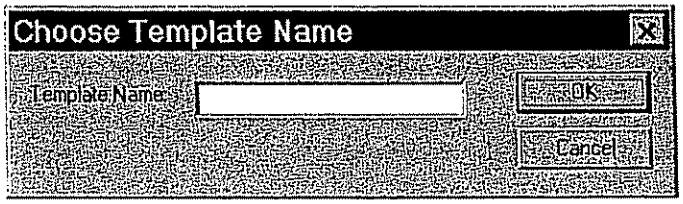


Figure 13: Choose Template Name dialog box

This dialog box sets a unique name for a new Template. Click the "Derive New Template" button on the Templates tab to access this dialog box

Type the new Template's name and click "OK."

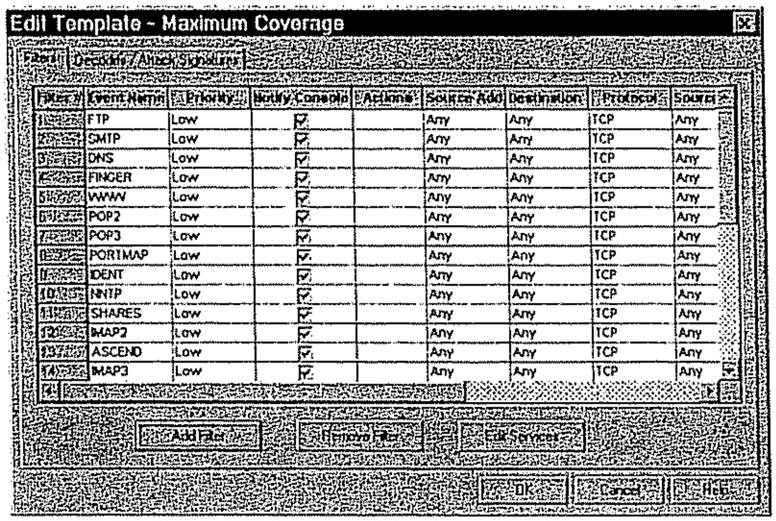
Note: *The new Template appears in the Templates window. To make changes to it, select it and click the "Customize" button to open the Edit Template dialog box.*

Configuring Templates

The Edit Template dialog box configures Templates for specific needs. To modify a Template, follow these steps:

1. In the Engine Properties dialog box, select the Templates tab.
2. Select the Template to modify. You may NOT edit a "Locked" Template. See also: "Derive New Template".
3. Click the "Customize" button. The Edit Template dialog box appears.

Edit Template Dialog Box



Filter #	Event Name	Priority	Notify Console	Actions	Source Add	Destination	Protocol	Source
1	FTP	Low	☑		Any	Any	TCP	Any
2	SMTP	Low	☑		Any	Any	TCP	Any
3	DNS	Low	☑		Any	Any	TCP	Any
4	FINGER	Low	☑		Any	Any	TCP	Any
5	WWW	Low	☑		Any	Any	TCP	Any
6	POP2	Low	☑		Any	Any	TCP	Any
7	POP3	Low	☑		Any	Any	TCP	Any
8	PORTMAP	Low	☑		Any	Any	TCP	Any
9	IDENT	Low	☑		Any	Any	TCP	Any
10	NNTP	Low	☑		Any	Any	TCP	Any
11	SHARES	Low	☑		Any	Any	TCP	Any
12	IMAP2	Low	☑		Any	Any	TCP	Any
13	ASCEND	Low	☑		Any	Any	TCP	Any
14	IMAP3	Low	☑		Any	Any	TCP	Any

Figure 14: Edit Template dialog box - Filters tab

The Edit Template dialog box is shown with the Filters tab selected.

Filters tab

The Filters tab displays the following parameters:

Filter #: A unique number that represents each filter in this Template. The filters are evaluated in this order.

***Note:** The order of filters is very important. Filters are evaluated in the order listed. Once a packet matches a filter, the filter process stops for the packet. If a packet matches multiple filters, only the first match will be found.*

Event Name: A brief name for each configurable filter in this Template. The Event name appears in the Management Console.

Priority: (configurable) The default priority for each filter is Low. Click in this box to set a different priority level. When the priority level is changed to Medium or High, it changes the window in which the events triggered by the filter are displayed in the RealSecure Console.

Notify Console: A check-box option determining whether or not the Engine notifies the Console when this filter is detected. If this option is checked, the detection information is displayed in the Console when a Console is running.

Actions: Click in this field to display a dialog box containing the actions that can be taken upon detection. For more information, see "Actions" later in this chapter.

Source Address: (configurable) The default source address for each filter is Any. Click in this box to invoke the "Enter Address" dialog box.

Destination: (configurable) The default destination for each source address is Any. Click in this box to invoke the "Enter Address" dialog box to specify an address.

Protocol: (configurable) Click in this box to choose a protocol (TCP, UDP or ICMP).

Source Port: (configurable) The default source port for each filter is "Any". Click in this box to define a specific address. This column is not used if the protocol is ICMP.

Destination: (configurable) The default destination for each source port is "Any". Click in this box to choose from a list of available source ports. This column is not used if the protocol is ICMP.

Type: This column is used only if ICMP is the selected protocol, select from the list of ICMP types. The protocol is ICMP. It indicates the value of the Type field from an ICMP packet. If you click in this box, you will be given a list of options.

Code: If ICMP is the selected protocol, select from the list of ICMP codes. This column is used only if the protocol is ICMP. It indicates the value of the Code field in an ICMP packet. If you click here, you will be given a list of options.

Buttons

Add Filter: Click this button to add a filter to this Template. An empty row is inserted before the highlighted row. If no row is highlighted, the cursor automatically moves to the bottom of the list and a new number is added. Enter the information for the new filter.

Remove Filter: Click this button to remove the selected filter from this Template. The numbers in the filter list are automatically corrected.

WARNING!

Use extreme caution when deleting filters. Do not delete a pre-configured filter, since these are used by the Attack Signatures to identify the type of attack.

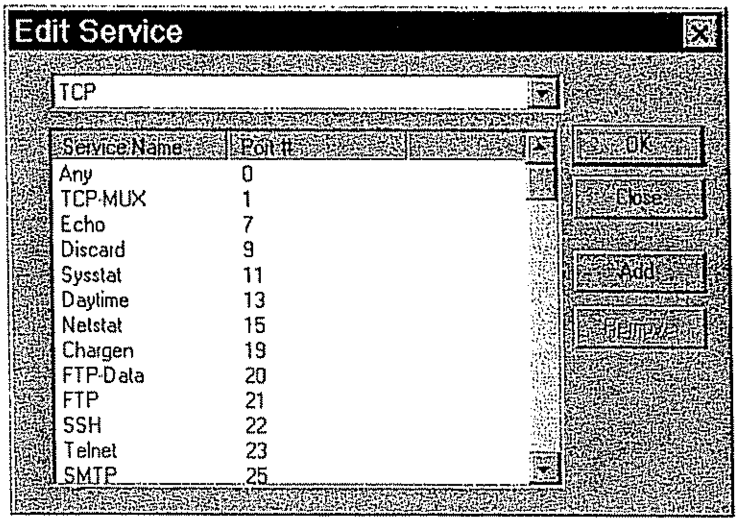
Edit Services: Displays the "Edit Service" dialog box.

OK: Saves changes and exits this dialog box.

Cancel: Exits without saving changes.

Help: Accesses the On-line Help topic for this tab.

Edit Service Dialog Box



Service Name	Port #
Any	0
TCP-MUX	1
Echo	7
Discard	9
Sysstat	11
Daytime	13
Netstat	15
Chargen	19
FTP-Data	20
FTP	21
SSH	22
Telnet	23
SMTP	25

Figure 15: Edit Service dialog box

This dialog box selects from a list of services associated with the selected filter.

- Choose a protocol from the drop-down list (TCP is shown).
- Select a service by highlighting an entry and clicking "OK".
- Add a new service to the list by clicking "Add".
- Remove a service from the list by selecting a service and clicking "Remove".

Buttons

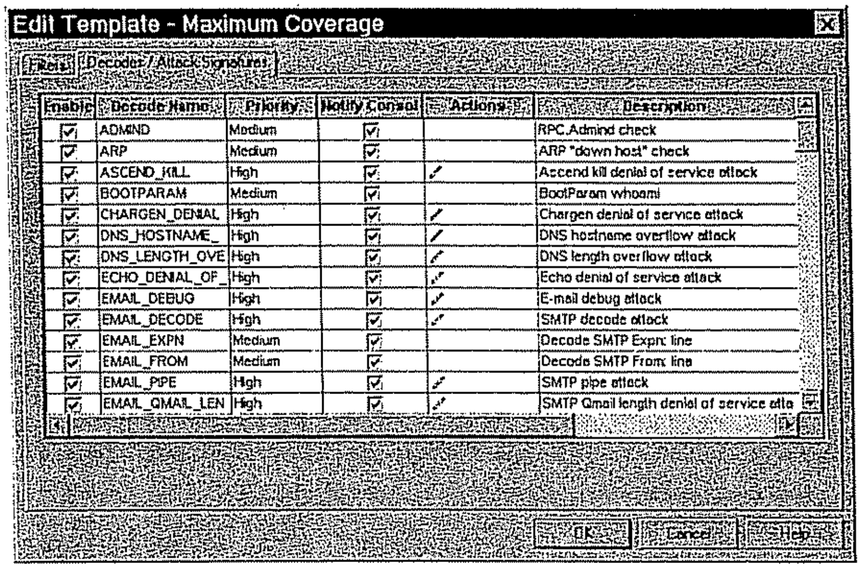
OK: Adds the selected service to the filter.

Close: Closes this dialog box without making any changes.

Add: Opens a dialog box that allows you to add a new service to the list.

Remove: Removes the selected service from the filter.

Decodes/Attack Signatures tab



Enable	Decode Name	Priority	Notify Consol	Actions	Description
☑	ADMIND	Medium	☑		RPC.Admind check
☑	ARP	Medium	☑		ARP "down host" check
☑	ASCEND_KILL	High	☑	✓	Ascend kill denial of service attack
☑	BOOTPARAM	Medium	☑		BootParam whoami
☑	CHARGEN_DENIAL	High	☑	✓	Chargen denial of service attack
☑	DNS_HOSTNAME_	High	☑	✓	DNS hostname overflow attack
☑	DNS_LENGTH_OVE	High	☑	✓	DNS length overflow attack
☑	ECHO_DENIAL_OF_	High	☑	✓	Echo denial of service attack
☑	EMAIL_DEBUG	High	☑	✓	E-mail debug attack
☑	EMAIL_DECODE	High	☑	✓	SMTP decode attack
☑	EMAIL_EXPN	Medium	☑		Decode SMTP Expn: line
☑	EMAIL_FROM	Medium	☑		Decode SMTP From: line
☑	EMAIL_PIPE	High	☑	✓	SMTP pipe attack
☑	EMAIL_QMAIL_LEN	High	☑	✓	SMTP Qmail length denial of service atta

Figure 16: Edit Template dialog box - Decodes/Signatures tab

The Decodes/Attack Signatures tab displays the following parameters:

Enable: A check box option which toggles the decode/attack signature on and off.

Decode Name: A brief name for each decode which can be detected by a Template. For more information, see Appendix A, "Attack Signatures."

Priority: (configurable) Click in this box to change the priority level of an attack. When the priority level changes, the window in which the Decode/Attack Signature is displayed in the RealSecure Console changes.

Notify Console: A check-box option which toggles whether or not the Engine notifies the Console when this decode/attack signature is detected If this option is checked, the event information is enabled and will display in the Console.

Actions: Click in this box to display a dialog box containing a list of available actions. For more information, see "Actions" later in this chapter.

Description: A brief description of the decode/attack signature For more information, see Appendix A, "Attack Signatures."

Options: (configurable) Some decodes/attack signatures have configurable parameters These are denoted by a gray push-button in this column. Click the gray button to display the Feature Options dialog box. If no configuration options are available for the selected decode/attack signature, this box displays "N/A" instead of a gray button.

Buttons

OK: Click this button to accept changes and close the dialog box.

Cancel: Click this button to exit this dialog box without applying changes

Help: Click this button to access an On-line Help topic for this tab.

Customizing Filters, Decodes and Attack Signatures

RealSecure is shipped with a substantial array of pre-defined attack signatures, session decodes, and filter rules The default Templates reflect combinations of these attacks, sessions, and filters for specific environments and purposes. These default Templates are guidelines, provided to begin using RealSecure as quickly as possible. Modify these Templates as appropriate for the network.

Note: *Default Templates are "Locked" and cannot be altered. If you want to create a customized Template, perform the following procedure:*

1. Select a Template to use as the bases for your customized Template.
2. Click "Derive New Template"
3. Name the new Template
4. Click the new template to highlight it

5. Click on Customize

You can add your own filter rules to RealSecure. RealSecure can be instructed to filter on any combination of the following:

- Protocol (TCP, UDP, ICMP)
- Source IP Address
- Destination IP Address
- Source Port
- Destination Port

Note: *You can specify a range of IP addresses using an address mask. More information about "Mask" and "Wildcards" to follow.*

How To Specify An IP Address

To access the "Enter Address" dialog, go to the Edit Template window, click on the Filters tab and click on the desired "Source Address" field.

The "Enter Address" dialog box will display.

This dialog is where you specify how many bits of the IP Address are significant. The larger the value specified, the more significant the IP Address.

How to use "Mask" and Using Wildcards

Examine the following IP Address

129.231.42.55

To run RealSecure against a specific IP Address only, enter the value 32 in the "Mask" field. Using the example IP Address above, to run RealSecure against the specific IP Address 129.231.42.55 only, enter 32 in the "Mask" field. Or, enter the numbers 129 as the first field value, 231 as the second, 42 as the third, and 55 as the last.

A value of 0 (zero) in the "Mask" field represents "Any". To enable the "Any" option, click in the checkbox named "Any Address". Or, simply enter the value 0 (zero) in the "Mask" field.

Note: *The "Any" option will disable all field values in the "Enter Address" dialog.*

A value of 8 is equivalent to a Class A network. For instance: To configure RealSecure to match all P Addresses in a Class A network, enter the value 8 in the "Mask" field. Using the example IP Address 129.231.42.55, you could enter 8 in the "Mask" field.

Note: 0 (zero) represents the lowest value and 32 represents the highest. Thus, the higher the value, the more significant the IP Address.

Use the following Address, Mask and Matches to determine valid field entries:

Address	***Mask***	***Matches***
129.231.42.55	*32*	*129.231.42.55*
129.231.42.55	*24*	*129.231.42.**
129.231.42.55	*16*	*129.231.*.**
129.231.42.55	*8*	*129.*.*.**
129.231.42.55	*0*	**.*.*.**

Note: You do not have to enter values in exact increments of 8 bits. Any number of bits beginning with 0 and ending with 32 are all valid entries in the "Mask" field.

Actions

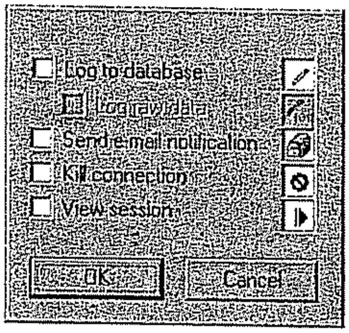


Figure 17: Actions dialog box

The Security Administrator can alter the actions that RealSecure takes when an attack or event is detected. These actions are set in the"Engine Properties" dialog box. To configure actions for a filter, click that filter's box in the "Actions" column of the Filters tab. The Actions dialog box is displayed. To configure actions for an attack signature session decode, click that attack signature box under the "Actions" column of the Attack Signatures/Decodes tab.

- **Log to Database:** Logs a summary of the event to the log database. When you upload the Engine Database to the console, you will be able to view (through the Session Playback window) the entire content of logged sessions.
- **Log raw data:** Log the entire binary content of a session to the log database (only available when "Log to Database" is checked)
- **Send e-mail notification:** Notifies the Security Administrator via e-mail when the specified event is detected.
- **Kill connection:** Kills the connection.

  How to Read the Kill

  A "Kill" may be read using either of the following methods:

  - Mask
  - Tree View

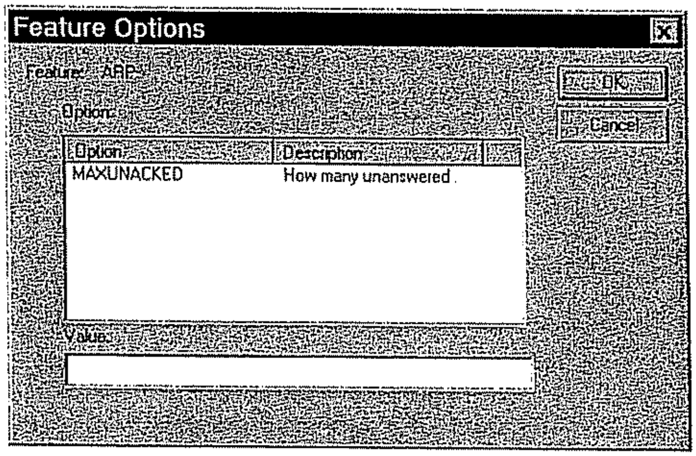
  Note: *It is important to protect all resources being attacked. If you want to determine who killed the connection, be aware that "Source" is not necessarily the identification of the person who killed the connection. To determine who killed the connection, you must know the user associated with the license Key of the machine that generated the "Kill".*

  Note: *This action applies only to TCP-based attacks. Use this option carefully, as it can seriously disrupt the flow of traffic on your network if misused. For example, if you set the kill option for a broad SMTP filter, you would terminate and prevent all e-mail sessions on your network and can have severe consequences on the performance of the network.*

  See also: Address Entry dialog box
  IP Spoofing

- **View session:** Allows you to view the session in real time. View session is similar to Log Raw in that it allows you to see the entire content of a session. However, data is passed up to the Management Console and is not stored in the database

Feature Options Dialog Box



Feature: ARP

Option:

Option	Description
MAXUNACKED	How many unanswered .

Value:

Figure 18: Feature Options dialog box

This dialog box appears when a configurable "Option" button is clicked in the Decodes/Attack Signatures tab of the Edit Template dialog box. The following items are available within this dialog box:

Feature: Displays the name of the selected decode/attack signature for configuration.

Option: Displays the name of the configuration option.

Description: A brief description of the selected option.

Value: Initially, this box is empty. Clicking on the option name displays information in the Value box. This information can be changed or replaced.

Note: *The value is not checked by RealSecure, and any errors can result in invalid signatures.*

Buttons

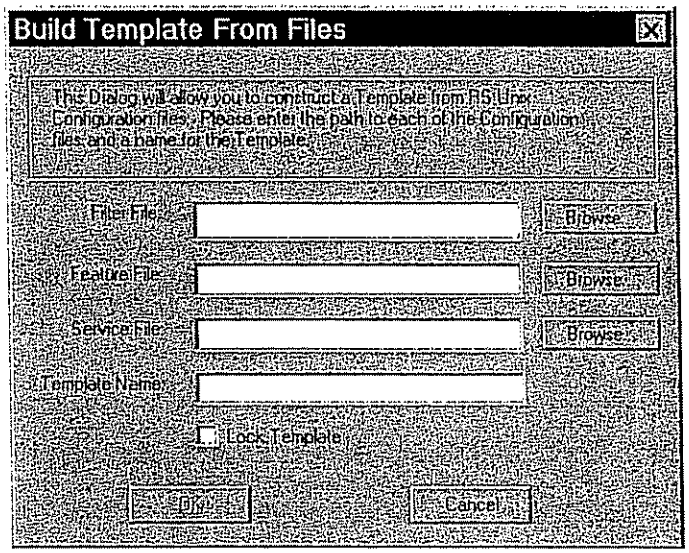
OK: Accepts changes and exit the dialog box.

Cancel: Exits from the dialog box without accepting any changes.

Importing UNIX Configuration Files as Templates

RealSecure for UNIX Templates can be used as Templates in RealSecure for Windows NT. This process can be accomplished by using the "Build Template From Files" dialog box.

Build Template From Files Dialog Box



This Dialog will allow you to construct a Template from RS Unix Configuration files. Please enter the path to each of the Configuration files and a name for the Template.

Figure 19: Build Template From Files dialog box

To access this dialog box, from the File menu select "Import UNIX RS Cfg Files." Templates created using this dialog box are automatically imported into RealSecure.

The following entries are required. All fields must be completed to continue with the exception of Lock Template.

Filter File: Enter the complete path to the UNIX Filter File, or click the "Browse" button to select a file This file is usually called "filter.cfg".

Feature File: Enter the complete path to the UNIX Feature File, or click the "Browse" button to select a file. This file is usually called "feature.cfg".

Service File: Enter the complete path to the UNIX Service File, or click the "Browse" button to select a file. This file is usually called "services".

Template Name: Type in a unique name for the new Template.

Lock Template: Check this box to prevent changes to the imported Template. To edit the Template after it has been imported, this check box must be cleared.

Buttons

OK: Click to accept the entries and import the UNIX configuration files as a Template.

Cancel: Click to exit this dialog box without importing UNIX files.

Browse: Searches for a directory path or file.

RealSecure™

Chapter 4: Using RealSecure for Windows NT

Now that you have installed RealSecure on your network and configured your Engines, you are ready to begin analyzing the data retrieved by the RealSecure Engines. This chapter discusses:

- The methods which RealSecure uses for Engine-Console communication.
- The RealSecure for Windows NT Management Console and how to use it.

Communicating with the RealSecure Management Console

The RealSecure Engines and the Management Console communicate using TCP and UDP. Data passed between the Engine and Console systems is encrypted and authenticated. The defaults are:

- TCP over port 139
- UDP over ports 900/901

Note: *The UDP port number can be changed, but not the TCP port.*

RealSecure can use different ports if these ports conflict with the current network setup.

Note: *Stop and restart the Engines and the Console after changing the listen ports.*

To change the Console Listen Port: Click the "Configuration Options" toolbar button, or select "Options" from the Console's View menu. This opens the Console Configuration dialog box. On the General tab, enter the new port number.

To change the Engine Listen Port: With an engine running, click the "View Engine Properties" toolbar button, or select "Properties" from the Engine menu in the Engines window. This opens the Engine Properties dialog box. On the General tab, enter the correct port number.

Engine -Console Communications

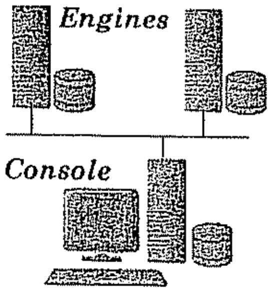


Figure 20. Engine to Console Communications

Once configured, the Engine no longer relies on the Console. The Console serves only as a configuration and viewing station. The Engine's local database runs autonomously without the Console.

The Engine's continue to log data into it's local database and performs all actions such as Kills and E-mails without the Console.

Note: *The only action that will not be seen are Events that have been marked as "View".*

The RealSecure Management Console accepts data from the RealSecure Engines in the following forms:

Event Messages: Indicates that something has occurred on the network. Event messages are passed to the Console as they occur, and appear in the Console's windows in real-time.

Raw Session Data: Select "Session Playback" from the Console's View menu to send each keystroke (or the data content of a session) to the Console as it occurs or from a logged session. The data content is displayed in the Session Playback window.

Database and Log File Information: This information is sent to the Console via an ODBC transaction over the network. Data is logged to an ODBC database. Data can then be retrieved and used by a variety of off-the-shelf packages, including report generators and decision support tools.

The Engine and Console have their own database instances even when they are on the same host.